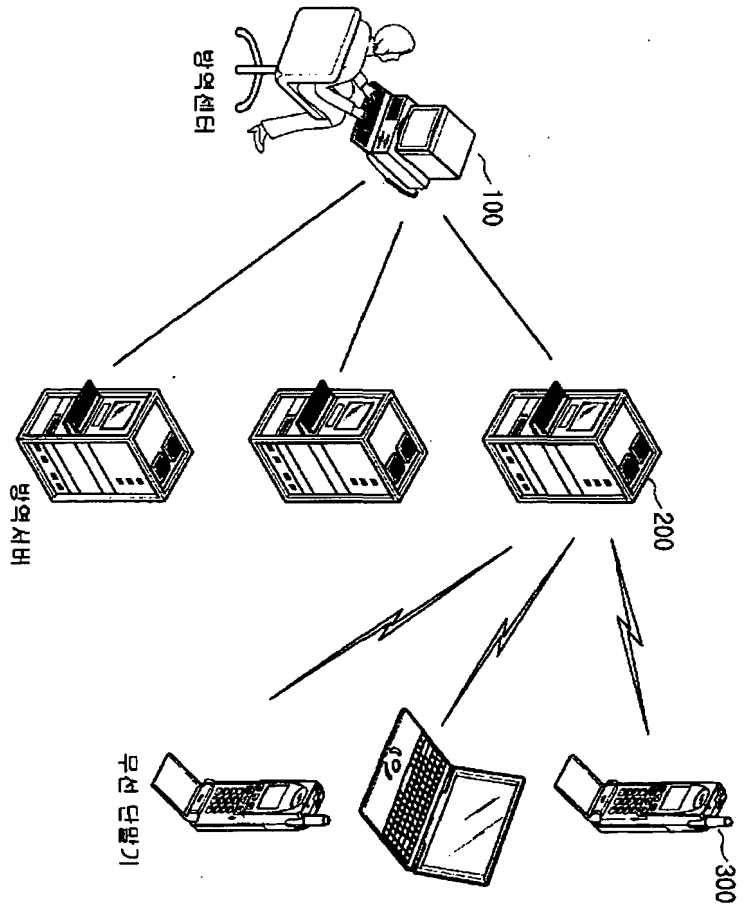
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020000063357 (43) Publication.Date. 20001106
(21) Application No.1020000036612 (22) Application Date. 20000629
(51) IPC Code:
G06F 11/00

(71) Applicant:
SECUI.COM CORPORATION
(72) Inventor:
KIM, DONG SIK
KIM, JEONG HWAN
(30) Priority:

(54) Title of Invention
SYSTEM AND METHOD FOR PREVENTING WIRELESS VIRUS

Representative drawing



(57) Abstract:

PURPOSE: A system and method for preventing wireless virus is provided to capture of the virus with use of a vaccine distribution system, automatically to prevent the virus in order to protect customer s information from the virus by providing an updated vaccine program.

CONSTITUTION: A user of a wireless terminal(300) such as a mobile phone, a smart phone, a PDA, a palm PC and an IMT2000 terminal is connected with a virus preventing server(200) through a WAP(Wireless Application Protocol) gateway. The virus preventing center(100) and the virus preventing server (200) are connected based on TCP/IP method. The virus preventing center(100) and the virus preventing server(200) may be connected based on a

Dynamic Host Configuration Protocol(DHCP) or a PPP method using a telephone line.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 11/00(조기공개)

(11) 공개번호 특2000-0063357
(43) 공개일자 2000년11월06일

(21) 출원번호 10-2000-0036612
(22) 출원일자 2000년06월29일

(71) 출원인 시큐아이닷컴 주식회사 오경수
서울특별시 강남구 역삼동 647-9 삼성역삼빌딩 17층

(72) 발명자 김동식
서울특별시강남구역삼동647-9삼성역삼빌딩17층

김정환
서울특별시강남구역삼동647-9삼성역삼빌딩17층

(74) 대리인 임평섭

심사청구 : 있음

(54) 무선 바이러스 방역 시스템 및 방역 방법

요약

고객의 무선 단말기 시스템을 실시간 모니터링하여 바이러스가 침입하는 즉시 바이러스 감시 및 백신 배포수단에서 이를 포착한 후 자동으로 바이러스를 방역하고, 업데이트된 백신을 배포함으로써 고객의 정보를 바이러스의 위험으로부터 안전하게 보호할 수 있으며, 신종 바이러스를 사전에 예방할 수 있도록 한 무선 바이러스 방역 시스템 및 방역 방법에 관한 것이다.

따라서, 무선으로 바이러스를 방역하는 방법은 무선 단말기 시스템에 바이러스가 발견되면 무선 단말기 내의 바이러스 진단 및 치료수단으로 상기 바이러스를 치료하는 단계와, 바이러스 진단 및 치료수단에 의해 바이러스의 치료가 불가능할 때 감염된 파일을 파일 전송 및 백신 배포수단을 통해 바이러스 감시 및 백신 배포수단으로 전송하는 단계와, 파일 전송 및 백신 배포수단으로부터 전송받은 감염 파일을 바이러스 감시 및 백신 배포수단에서 분석한 후, 업데이트된 백신을 개발하여 모든 파일 전송 및 백신 배포수단에 배포하는 단계, 및 파일 전송 및 백신 배포수단에서 업데이트된 백신을 모든 무선 단말기로에 배포하는 단계로 달성할 수 있다.

대표도

도1

색인어

무선 단말기, 바이러스, 방역 시스템, 인터넷, 백신, 모니터링

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 무선 인터넷 바이러스 방역 시스템의 개략도이다.

도 2는 본 발명에 따른 방역센터를 나타내는 구성도이다.

도 3은 본 발명에 따른 방역서버를 나타내는 구성도이다.

도 4는 본 발명에 따른 무선 단말기를 나타내는 구성도이다.

도 5는 본 발명에 따른 무선 바이러스 방역 시스템의 전체 흐름도이다.

<도면의 주요 부분에 대한 부호의 설명>

100 : 바이러스 감시 및 배포수단(방역센터)

200 : 파일 전송 및 배포수단(방역서버)

300 : 무선 단말기 102 : 센터 콘솔

104 : 센터서버 모듈 106 : 소프트 콘솔

202 : 사이트서버 모듈 204 : 사이트 콘솔

302 : 소프트 클라이언트 303 : 바이로봇

304 : 램상주 바이로봇 306 : 디스크 바이로봇

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 무선 통신망을 이용한 무선 바이러스 방역 시스템 및 그 방법에 관한 것으로, 상세하게는 무선 통신망을 이용하여 원격으로 무선 단말기 시스템을 실시간으로 모니터링하여 무선 단말기 시스템에 바이러스가 침입하는 즉시 바이러스 감시 및 백신 배포수단에서 이를 포착하여 자동으로 바이러스를 방역하는 무선 통신망을 이용한 무선 바이러스 방역 시스템 및 그 방법에 관한 것이다.

최근 들어 폭발적으로 활성화되어 유용한 정보를 얻을 수 있는 방법으로 유선으로 정보를 제공하는 유선 인터넷과 무선으로 정보를 제공하는 무선 인터넷 및 무선 이동통신을 들 수 있다. 또한 무선으로 정보를 제공하는 무선 인터넷 및 무선 이동통신은 기술의 발달로 서로의 특징을 하나로 결합되는 경향을 보이고 있다.

현재 무선으로 인터넷을 수행할 수 있는 휴대폰, 스마트폰, PDA, 팜PC 및 IMT2000(International Mobile Telecommunications-2000) 단말기 등의 무선 단말기들은 대용량의 메모리를 쓰게 됨에 따라서 각 메모리를 관리하기 위한 파일 시스템을 기본적으로 내장하게 되고, 기존의 유선 컴퓨터와 유사하게 이메일을 이용하여 자료를 교환하거나 인터넷 서비스로서 정보를 검색하는 등의 외부 자료와의 접촉이 현저하게 증가하고 있다. 그러나, 이러한 외부 자료와의 접촉은 수신되는 여러가지 정보 및 프로그램들을 통하여 바이러스에 노출될 수 있으며, 현재 무선 단말기에 대한 바이러스 피해를 예방할 수 있는 방법이 미비하였다.

따라서, 무선 단말기를 유선 컴퓨터와 같이 바이러스를 체크하여 방역할 수 있으며, 업데이트된 새로운 백신을 제공할 수 있는 것이 필요하였다.

발명이 이루고자하는 기술적 과제

따라서, 본 발명은 상기한 문제점을 해결하기 위한 것으로 본 발명의 목적은 원격으로 고객의 무선 단말기 시스템을 실시간 모니터링하여 바이러스가 침입하는 즉시 바이러스 감시 및 백신 배포수단에서 이를 포착한 후 자동으로 바이러스를 방역함으로써 고객의 정보를 바이러스의 위험으로부터 안전하게 보호할 수 있는 무선 바이러스 방역 시스템 및 그 방법을 제공하는 것이다.

본 발명의 다른 목적은 실시간 분석을 통해 신종 바이러스를 빠른 시간 내에 분석한 후, 모든 무선 단말기에 자동으로 백신을 배포함으로써 신종 바이러스가 침투하는 것을 사전에 예방할 수 있는 무선 바이러스 방역 시스템 및 그 방법을 제공하는 것이다.

본 발명의 또 다른 목적은 고객에게 백신을 푸신 방식 또는 풀 방식을 겸용하여 배포하는 무선 바이러스 방역 시스템 및 그 방법을 제공하는 것이다.

발명의 구성 및 작용

상기 목적을 달성하기 위한 본 발명의 무선 바이러스 방역 시스템은 센터서버 모듈(Center Server Module), 센터 콘솔(Center Console) 및 소프트 콘솔(Soft Console)로 이루어진 바이러스 감시 및 백신 배포 수단(이하, 방역센터라 함)과, 사이트서버 모듈(Site Server Module)과 사이트 콘솔(Site Console)로 이루어진 파일 전송 및 백신 배포수단(이하, 방역서버라 함)과 바이로봇(Virobot)과 소프트 클라이언트(Soft Client)로 이루어진 무선 단말기로 구성된 것을 특징으로 한다.

센터서버 모듈은 소프트 콘솔에서 업데이트된 백신을 전송받아 각 사이트서버 모듈에 풀(pull) 방식으로 전송하고, 전송 실패시 부시(push)방식으로 배포하는 것을 특징으로 한다.

센터 콘솔은 무선 단말기로부터 전송받은 로그/이벤트 기록 등의 정보를 수집하여 실시간으로 무선 단말기의 시스템을 모니터링하는 것을 특징으로 한다.

사이트서버 모듈은 센터서버 모듈에서 제공받은 업데이트된 백신을 무선 단말기에 풀 또는 푸시 방식으로 배포하는 것을 특징으로 한다.

또한 본 발명에 의한 무선 바이러스 방역 시스템의 방역 방법은 무선 단말기 시스템에 바이러스가 발견되면 무선 단말기내의 바이러스 진단 및 치료수단으로 상기 바이러스를 치료하는 단계와, 바이러스 진단 및 치료수단에 의해 바이러스의 치료가 불가능할 때 감염된 파일을 파일 전송 및 백신 배포수단을 통해 바이러스 감시 및 백신 배포수단으로 전송하는 단계와, 파일 전송 및 백신 배포수단으로부터 전송받은 감염 파일을 바이러스 감시 및 백신 배포수단에서 분석한 후, 업데이트된 백신을 개발하여 모든 파일 전송 및 백신 배포수단에 배포하는 단계, 및 파일 전송 및 백신 배포수단에서 업데이트된 백신을 모든 무

선 단말기로에 배포하는 단계로 달성할 수 있다.

이하; 첨부된 도면을 참조하면서 상세히 설명하기로 한다.

도 1은 본 발명에 따른 무선 바이러스 방역 시스템의 개략도이고, 도 2는 본 발명에 따른 방역센터를 나타내는 구성도이며, 도 3은 본 발명에 따른 방역서버를 나타내는 구성도이고, 도 4는 본 발명에 따른 무선 단말기를 나타내는 구성도이다.

본 발명에 따르면, 휴대폰, 스마트폰, PDA, 팜PC 및 IMT2000 단말기 등의 무선 단말기(300) 사용자는 WAP(Wireless Application Protocol) 게이트웨이를 통하여 방역서버(200)에 접속되며, 방역센터(100)와 방역서버(200)는 일반적으로 TCP/IP 방식으로 연결되나 방역서버(200)의 요청으로 인하여 어드레스 자동 취득 프로토콜(Dyanmic Host Configuration Protocol; 이하, DHCP라 함) 방식 또는 전화선을 이용한 PPP 방식으로도 연결될 수 있다.

도 2에 도시한 바와 같이 방역센터(200)는 센터서버 모듈(104), 센터 콘솔(102) 및 소프트 콘솔(106)을 포함한다.

센터서버 모듈(104)은 방역서버(200)로부터 수신된 무선 단말기(300)의 로그/이벤트 기록 등의 정보를 데이터 베이스화하여 센터 콘솔(102)로 전송한다. 또한 센터서버 모듈(104)을 방역서버(200)로부터 전송받은 바이러스 감염 파일을 소프트 콘솔(106)로 전송하여 분석을 의뢰하고, 소프트 콘솔(106)에서 분석하여 업데이트된 백신을 전송받아 각각의 방역서버(200)에 풀 또는 푸시 방식으로 배포한다. 이때, 센터서버 모듈(104)은 각각의 방역서버(200)와 암호를 통하여 통신을 하게 되는데 그 중의 하나는 공개키 기반구조(Public Key Infrastructure) 방식으로 통신을 하는 것이다.

센터 콘솔(102)은 고객으로부터 전송받은 각종 로그/이벤트 기록 등의 정보를 수집하여 실시간으로 무선 단말기(300)의 시스템을 모니터링한다. 이때, 무선 단말기(300)에서 신종 바이러스가 발견되면 즉시 대응이 가능하도록 방역서버(200)에 음향, 호출기, 휴대폰 및 단문 메시지 서비스(Short Message Service; 이하 SMS라 함) 등의 경고수단으로 알려주게 된다. 또한 센터 콘솔(102)은 사이트서버 모듈(202)과의 대화 내역 등을 기록하기 위한 채팅 기능을 추가할 수 있다.

소프트 콘솔(106)은 센터서버 모듈(104)로부터 전송받은 바이러스 감염 파일을 빠른 시간내에 분석하고, 분석된 업데이트 백신을 센터서버 모듈(104)로 다시 전송한다.

도 3에서 도시한 바와 같이 방역서버(200)는 사이트서버 모듈(202)과 사이트 콘솔(204) 및 WAP 게이트웨이(206)를 포함한다

사이트서버 모듈(202)은 각 무선 단말기(300)의 로그/이벤트 기록 등의 정보 및 바이러스 감염된 파일을 방역센터(100)로 전송한다. 또한 사이트서버 모듈(202)은 주기적으로 방역센터(100)를 조회하여 최신의 업데이트 백신을 다운로드 받아 모든 고객의 무선 단말기(300)에 풀 또는 푸시 방식으로 업데이트 백신을 배포한다.

사이트 콘솔(204)은 사이트서버 모듈(202)에 접속하여 무선 단말기(300)로의 업데이트 배포 상황과 바이러스 현황을 모니터링한다. 또한 사이트 콘솔(204)은 무선 단말기(300)에 바이러스가 발견되면 무선 단말기에 음향, 호출기, 휴대폰, SMS 등의 경고수단으로 알려주게 된다.

도 4에서 도시한 바와 같이 본 발명의 무선 단말기는 소프트 클라이언트(302)와 바이로봇(303) 등을 포함한다.

바이로봇(303)은 램상주 바이로봇(304), 디스크가 존재할 때에는 디스크 바이로봇(306)을 포함하고, 바이러스를 진단하고 치료하는 기능을 수행하며, 그 결과를 소프트 클라이언트(302)에 전송한다. 램상주 바이로봇(304)은 항상 램에 상주하여 파일, 압축파일을 실행할 때 바이러스를 진단하여 치료한다.

소프트 클라이언트(302)는 바이로봇(303)으로부터 전송받은 바이러스의 진단결과와 바이러스에 감염된 파일을 방역서버(200)로 전송하고 바이로봇(303)의 패치 등을 수행하여 방역서버(200)로부터 명령을 전달받아 보안을 책임진다.

이하, 본 발명의 동작을 도 5의 흐름을 통하여 상세하게 설명한다.

방역 서비스가 실시되는 무선 단말기에 전원이 들어오면(단계 S502), 램상주 바이로봇(304)의 백신 프로그램이 작동하여 현재 메모리에 있는 감염 가능한 파일을 검사한다(단계 S504). 이때, 감염된 파일을 정상적으로 회복시키지 못한 경우 소프트 클라이언트(302)에 해당 메시지를 전달한 후 사이트서버 모듈(202)로 감염된 파일을 전송한다.

파일 검사후 무선 단말기가 현재 갖고 있는 백신의 정보를 방역서버(200)의 사이트 서버 모듈(202)에 넘겨주어 업데이트의 필요 여부를 판단한다(단계 S508). 이 때, 업데이트의 필요가 있으면 방역서버(200)에서 새로운 백신을 페이징으로 업데이트를 하거나 또는 고객에서 업데이트의 필요성을 지적하여 트래픽 채널(traffic channel)로 업데이트를 한다(단계 S510).

무선 단말기(300)를 통하여 고객이 프로그램을 다운로드 받거나 이메일(e-mail)을 사용할 때 메모리를 액세스(access)하게 되면(단계 S514) 무선 단말기(300) 내의 바이로봇(303)에 의해 백신으로 해당 파일을 진단한다(단계 S516).

또한 무선 단말기(300)의 전원을 다운(down)되면 off하는 경우에 메모리에 있는 모든 파일을 백신으로 진단한다(단계 S520).

다음에는 무선 바이어스 방역 시스템에 장애가 발생할 경우에 대하여 그 대처 방안을 예를 들어 설명한다.

첫째, 방역센터(100) 시스템이 다운되었을 경우, 방역서버(200)는 방역센터로 보낼 각종 정보를 방역서버(200)의 로컬 디렉토리(Local Directory)(206)에 저장하였다가 방역센터(100)와의 교신이 이루어질 경우 일괄적으로 전송하고 삭제한다. 로컬 디렉토리(206)에 저장될 정보는 시간대 별로 순서화 되어 전송되고 또한 순차적으로 방역센터로 전송된다.

둘째, 방역서버(200)의 시스템이 다운되었을 경우에, 방역센터(100)는 정상적으로 교신이 이루어지는 다른 방역서버(200)에만 데이터를 전송한다. 그러므로 다운된 방역서버(200)의 관리하에 있는 모든 무선 단말기(300)의 레지스트리에 계속적으로 로그 기록 및 감염 파일의 정보를 저장하게 되고, 교신이 이루어지면 방역서버(200)에 저장된 정보를 전송하고 레지스트리에서 로그 기록을 삭제한다.

셋째, 무선 단말기(300)의 메모리가 꽉 차게 되어 패치가 어려울 경우에, 무선 단말기 사용자에게 이러한 상황을 먼저 알린 후 사용 가능한 공간을 확보하도록 유도한다. 소프트 클라이언트(302)는 사용자의 단말기에서 항상 가장 많이 남아 있는 메모리를 다운 디렉토리로 지정하게 된다. 또한 메모리의 변화가 발생하면 자동으로 다운 디렉토리를 생성한다.

발명의 효과

이상 설명한 바와 같이, 본 발명에 의한 무선 바이러스 방역 시스템 및 그 방법은 무선을 통해 원격으로 고객의 무선 단말기 시스템을 실시간으로 모니터링하여 바이러스가 침입하는 즉시 방역센터에서 이를 포착한 후 자동으로 바이어스를 방역함으로써 고객의 정보를 내외부의 위험으로부터 안전하게 보호할 수 있는 효과가 있다.

또한 본 발명은 업데이트된 백신을 고객 단말기에 자동으로 배포함으로써 바이러스의 공포로부터 완전히 해소될 수 있는 효과가 있다.

또한 메시지 기능이 내장되어 있으므로 관리자가 전체 사용자 또는 특정 사용자에게 메시지를 보낼 수 있어 바이러스에 대한 정보를 손쉽게 전달할 수 있다.

이상 설명한 내용을 통해 당업자라면 본 발명의 기술적 사상을 벗어나지 않는 범위에서 다양한 변경 및 수정이 가능함을 알 수 있을 것이다. 따라서, 본 발명의 기술적 범위는 첨부한 도면과 명세서의 상세한 설명에 기재된 내용으로 한정되는 것은 아니다.

(57) 청구의 범위

청구항 1

무선 단말기의 바이러스를 방역하는 시스템에 있어서

상기 바이러스가 침입하면 바이러스 진단 및 치료수단으로 상기 바이러스를 치료하고, 치료하지 못한 파일은 파일 전송 및 백신 배포수단에 전송하는 무선 단말기와;

상기 무선 단말기로부터 전송된 감염 파일을 바이러스 감시 및 백신 배포수단으로 전송하며, 업데이트된 백신을 상기 무선 단말기에 배포하는 파일 전송 및 백신 배포수단; 및

상기 바이러스의 침입여부를 모니터링하고, 상기 감염된 파일을 상기 파일 전송 및 백신 배포수단으로부터 전송받아 백신을 업데이트하며, 상기 업데이트된 백신을 모든 파일 전송 및 백신 배포수단에 배포하는 바이러스 감시 및 백신 배포수단을 구비함을 특징으로 하는 무선 바이러스 방역 시스템.

청구항 2

제 1 항에 있어서, 상기 바이러스 감시 및 백신 배포수단은

상기 무선 단말기에 바이러스의 침입 여부를 모니터링 하는 센터 콘솔과;

상기 업데이트된 백신을 모든 파일 전송 및 백신 배포수단으로 전송하는 센터서버 모듈과;

상기 바이러스에 감염된 파일을 분석한 후 업데이트된 백신을 개발하여 상기 센터서버 모듈로 전송하는 소프트 콘솔을 포함하는 것을 특징으로 하는 무선 바이러스 방역 시스템.

청구항 3

제 1 항에 있어서, 상기 파일 전송 및 백신 배포수단은,

상기 바이러스 감시 및 백신 배포수단으로부터 수신된 업데이트된 백신을 상기 무선 단말기에 배포하는 사이트서버 모듈과;

상기 바이러스가 발견되면 상기 무선 단말기에 경고하여 알려주는 사이트 콘솔을 포함하는 것을 특징으로 하는 무선 바이러스 방역 시스템.

청구항 4

제 1 항에 있어서, 상기 무선 단말기는

상기 바이러스를 진단 및 치료하는 바이로봇과;

상기 바이러스의 진단 결과와 상기 바이러스에 감염된 파일을 상기 파일 전송 및 백신 배포수단으로 전송하는 소프트 클라이언트를 포함하는 것을 특징으로 하는 무선 바이러스 방역 시스템.

청구항 5

제 4 항에 있어서, 상기 바이로봇은

램에 상주하여 파일을 실행할 때 상기 바이러스를 진단하고 치료하는 램상주 바이로봇과;

일정 시간마다 무선 단말기의 모든 파일을 검사하는 디스크 바이로봇을 포함하는 것을 특징으로 하는 무선 바이러스 방역 시스템.

청구항 6

무선 단말기 시스템에 바이러스가 발견되면 상기 무선 단말기내의 바이러스 진단 및 치료수단으로 상기 바이러스를 치료하는 단계;

상기 바이러스 진단 및 치료수단에 의해 바이러스의 치료가 불가능할 때 상기 감염된 파일을 파일 전송 및 백신 배포수단을 통해 바이러스 감시 및 백신 배포수단으로 전송하는 단계;

상기 파일 전송 및 백신 배포수단으로부터 전송받은 상기 감염 파일을 바이러스 감시 및 백신 배포수단에서 분석한 후, 업데이트된 백신을 개발하여 모든 파일 전송 및 백신 배포수단에 배포하는 단계; 및

상기 파일 전송 및 백신 배포수단에서 상기 업데이트된 백신을 모든 무선 단말기로에 배포하는 단계로 이루어진 것을 특징으로 하는 무선 바이러스 방역 방법.

청구항 7

제 6 항에 있어서, 상기 바이러스 감시 및 백신 배포수단과 파일 전송 및 백신 배포수단은 TCP/IP 방식, 어드레스 자동 취득 프로토콜 방식 및 전화선을 이용한 PPP 방식 중의 하나로 연결되는 것을 특징으로 하는 무선 바이러스 방역 방법.

청구항 8

제 6 항에 있어서, 상기 바이러스 감시 및 백신 배포수단의 시스템 다운(system down)으로 인하여 파일 전송 및 백신 배포수단에서의 전송이 불가능한 경우에 있어서,

상기 파일 전송 및 백신 배포수단의 로컬 디렉토리에 상기 무선 단말기로부터 전송된 로그 기록 및 감염 파일의 정보를 시간대별로 순서화하여 저장하고, 상기 바이러스 감시 및 백신 배포수단과의 통신이 이루어지면 상기 파일 전송 및 백신 배포수단의 로컬 디렉토리에 저장되어 있는 정보를 순차적으로 전송한 후 삭제하는 것을 특징으로 하는 무선 바이러스 방역 방법.

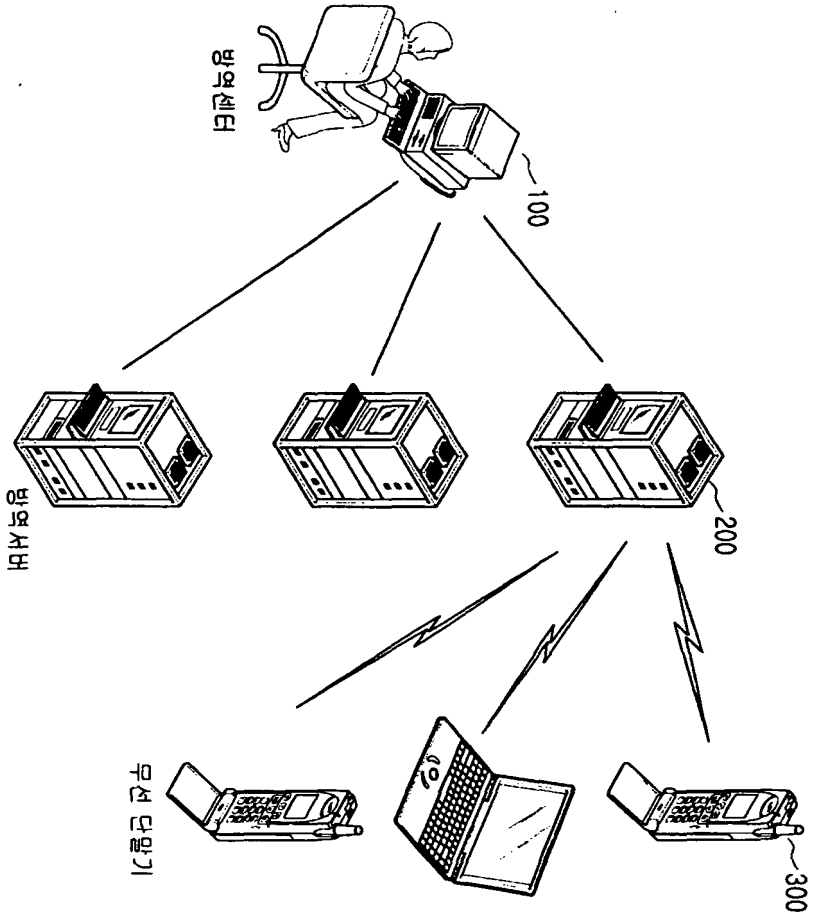
청구항 9

제 6 항에 있어서, 상기 파일 전송 및 백신 배포수단의 시스템 다운으로 인하여 무선 단말기의 정보를 전송할 수 없는 경우에 있어서,

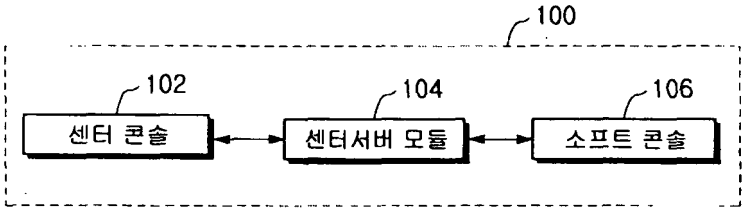
상기 무선 단말기의 레지스트리에 로그 기록 및 감염 파일의 정보를 순차적으로 저장하고, 상기 파일 전송 및 백신 배포수단과의 통신이 이루어지면 파일 전송 및 백신 배포수단으로 상기 로그 기록 및 감염 파일의 정보를 순차적으로 전송한 후 삭제하는 것을 특징으로 하는 무선 바이러스 방역 방법.

도면

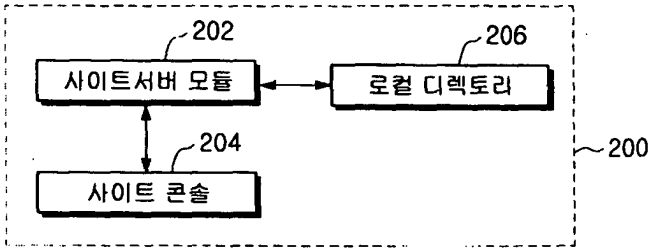
도면1



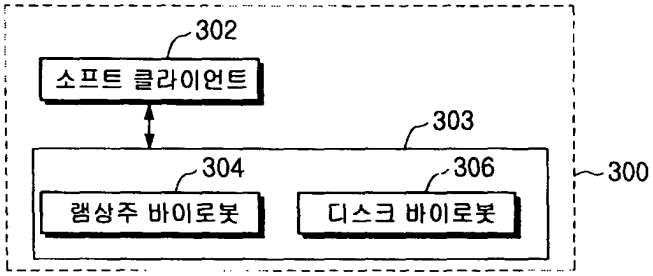
도면2



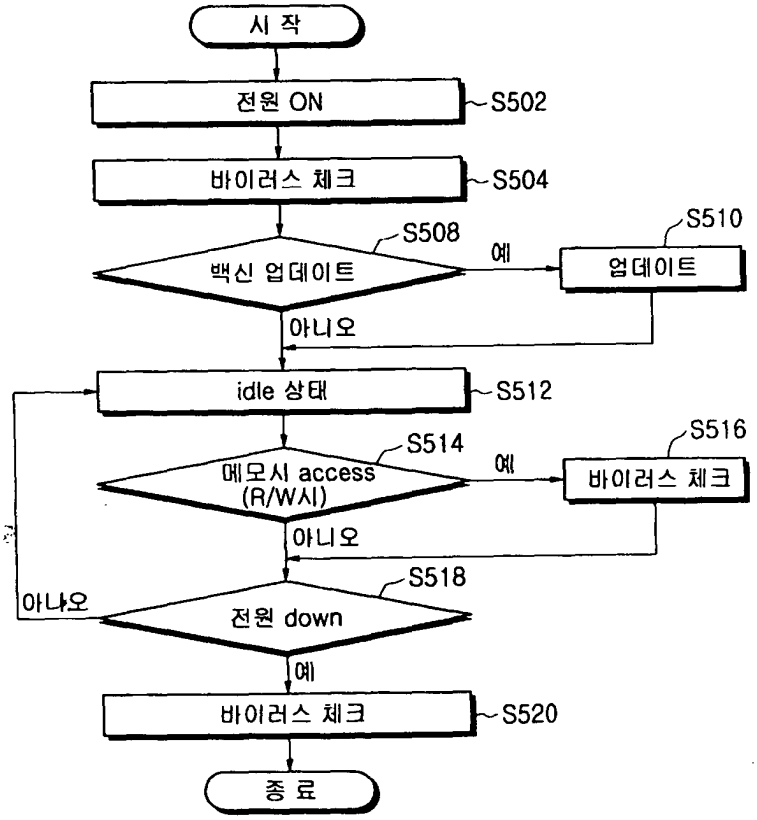
도면3


202
206
사이트서버 모듈
로컬 디렉토리
204
200
사이트 콘솔

도면4


302
소프트 클라이언트
303
304
306
300
램상주 바이로봇
디스크 바이로봇

도면5


시 작
전원 ON
S502
바이러스 체크
S504
S508
S510
백신 업데이트
예
업데이트
아니오
idle 상태
S512
S514
S516
메모시 access
(R/W시)
예
바이러스 체크
아니오
S518
아니오
전원 down
예
바이러스 체크
S520
종 료